Schedule 9

Security Services

to

Request for Proposal
for the
Provision of IT Infrastructure Operations
and Managed Workplace Services
[UNHCR RFP/2018/1068]
(the “RFP”)

effective _____ 2018

between

The Office of the United
Nations High Commissioner
for Refugees

and Contractor

Table of Contents

1 INTRODUCTION 3
2 SERVICES 3
3 IMPLEMENTATION OF SECURITY SERVICES 7
4 OUT OF SCOPE SECURITY SERVICES 8

1 Introduction

1.1. This Schedule 9 sets forth Contractor's roles and responsibilities in providing security support services to systems and Users at all UNHCR locations.

1.2. Unless the context otherwise requires, capitalized terms used but not defined in this Schedule 9 shall have the meaning given to them in Schedule 1 (Technical Definitions) or the Agreement.

2 Services

2.1. General

Security Services are the functions associated with maintaining physical and logical security for in-scope Services components (e.g., Software, Data, Hardware) in compliance with UNHCR Security policies and requirements.

The following are the key high-level Service objectives UNHCR expects to achieve through outsourced Security Services:

- Maintain best practices for delivery of the Security Services and implement a service delivery program that comports with those practices;
- Provide Security Services with guarantees backed by Service Level Requirements (SLRs);
- React to and resolve all security incidents derived from events and alerts raised by external Managed Security Services, internal Security Information and Event Management (SIEM) tools and from other Third-Parties;
- Provide Security Services with features and functions that meet User needs and meet UNHCR business requirements; and
- Cost-effectively maintain and support UNHCR Security infrastructure with appropriately skilled staff to meet established Service Level Requirements.

Contractor shall provide both remote and on-site security services as required to servers, workstations, and devices by following ITIL Service Management processes and as per guidelines and policies as defined or agreed by UNHCR. The sub-services as more fully described in this Section 2 include:

(a) security practices;

(b) security patching;

(c) malware prevention, response, mitigation and service restoration;

(d) Security Operations Center (SOC), monitoring and incident management;

(e) system administrative privilege support; and

(f) security assessment and audit support.

2.2. Personnel

Providing trained and qualified personnel is essential to effective service delivery.

Contractor shall:

(a) Provide personnel with technical skills and competencies that allow for effective delivery of Services;

(b) understand ITIL processes of incident, problem, change, release & deployment, asset and configuration management;

(c) be familiar with techniques of on-site customer interaction and high standards of customer support;

(d) be familiar with UNHCR standard endpoint devices, standard operating environments, and standard image software;

(e) understand the UNHCR service level agreement and prioritization of Incidents and Service Requests;

(f) have been on-boarded with knowledge of the UNHCR business, mission, security awareness, and policies;

(g) understand the requirements and obligations of the UNHCR Data Protection Policy;

(h) understand the requirements and obligations of the UNHCR Administrative Instruction on Access Controls; and

(i) understand the requirements and obligations of the UNHCR Administrative Instruction on ICT Security.

2.3. System Practices

System Practices are those activities associated with the continual planning, awareness, and training towards effective system security.

Contractor Shall:

(a) Adhere to UNHCR security policies and requirements for protecting UNHCR systems and data, including the Policy on the Protection of Personal Data of Persons of Concern to the UNHCR (Data Protection Policy);

(b) designate a security officer to work with the UNHCR on system security practices, requirements and activities;

(c) train all Contractor personnel supporting UNHCR systems on information security awareness;

(d) ensure Contractor personnel are aware of security trends, threats, common exploits, and security best practices;

(e) put in place, and maintain, physical and logical managed services security controls consistent with industry best practices (such as ISO 27001, COBIT 5) and UNHCR security policies;

(f) document adherence to security policies, practices, and requirements in managed services activities;

(g) protect UNHCR systems and data, logically and physically, when in use, at rest, and during transmission against unauthorized access or modification, in accordance with the Agreement;

(h) designate a focal point for coordination of Data Centre access and badging; and

(i) provide and maintain the list of Contractor personnel with access to UNHCR systems for regular reporting, review, and approval.

2.4. Security Patching

Security Patching Services are those activities associated with maintaining workstations and servers to mitigate Software/OS security vulnerabilities.

Contractor Shall:

(a) Collaborate with UNHCR to define and maintain policies related to Software/OS and security patch deployment and severity levels;

(b) comply with UNHCR practices and policies related to Software/OS version control and patch management;

(c) identify Software/OS and security patches relevant to the Data Centre and Decentralized environments, inclusive of servers, storage and network devices, and classify patches based on agreed policies and procedures;

(d) identify Software/OS and security patches relevant to workstations and User environments and classify patches based on agreed policies and procedures;

(e) prepare and maintain a security patch deployment plan for servers and workstations for UNHCR review and approval; and

(f) deploy and install Software/OS security patches in accordance with agreed UNHCR Change Control Procedure.

2.5. Malware Prevention, Response, Mitigation, and Restoration

Malware Prevention, Response and Mitigation Services are those activities associated with planning, protection and mitigation of malware and virus outbreaks from workstations and servers.

Contractor Shall:

(a) Collaborate with UNHCR and other UNCHR Managed Security Services providers in creating an established action plan in the case of malicious code outbreak;

(b) install, configure, and operate malware protection software on in-scope service environment devices, where possible, for continuous scanning, eradication, and reporting of detected malware and malware Incident resolution;

(c) deploy anti-virus and anti-malware updates and patches per the UNHCR patch, change, and release and deployment management procedures;

(d) provide automated detection and removal of malicious code using anti-malware software;

(e) monitor systems for malicious code outbreaks;

(f) provide regular updates of the antivirus signature files on systems;

(g) promptly notify UNHCR on detection of malicious code within the UNHCR ICT environment;

(h) execute agreed action plans and escalation procedures for a malicious code outbreak; and;

(i) be responsible for restoration of service through mitigation and removal of malware and viruses from impacted workstations and servers.

2.6. Security Operations Center, Monitoring, and Incident Management

Security Operations Center (SOC), Security Monitoring and Security Incident Management Services are those activities associated with the planning, monitoring, identification, and response to security incidents.

Contractor Shall:

(a) Provide Security Operation Center (SOC) services to centralize the monitoring, communications, management, and mitigation of security issues;

(b) work with UNHCR and other UNCHR Managed Security Services providers to establish security and incident response procedures;

(c) manage and maintain UNHCR security monitoring tools;

(d) perform 24x7 security log monitoring, analysis, triage, and Incident alerting from the UNHCR network, data centers, and security environment,

(e) receive and react to events and alerts received from Third Parties;

(f) notify UNHCR of any Incident or suspected Incident related to:

(i) Unauthorized access to UNHCR systems or Data;

(ii) unauthorized (intentional or accidental) dissemination of UNHCR Data;

(iii) malicious code activity, including Trojans, root kits, backdoors, bots or any malware suspected of compromising UNHCR Data;

(iv) any other activities indicating potential security breaches that may result in the loss of UNHCR Data.

(g) collaborate with UNHCR personnel to respond to and resolve all security Incidents following triage and severity assignment;

(h) define and perform security on-boarding process for servers, workstations and devices;

(i) provide reporting that correlates event data to threats identified;

(j) provide vulnerability scan and analysis on a recurring and per-request basis, categorize and prioritize scan results by risk;

(k) provide URL filtering, monitoring, and reporting;

(l) participate in the UNHCR security incident response process, including security event planning, response preparation, and event response activities; and

(m) report security risks and security incidents to the UNHCR ICT Security Officer in accordance with UNHCR security policies.

2.7. System Administrative Privilege Support

System Administrative Privilege Support Services are those activities associated with maintaining accounts for users with elevated privileges (e.g. admin, root, etc.).

Contractor Shall:

(a) Maintain a registry of all Contractor and UNHCR accounts with administrative-level privileges for all in-scope platforms (e.g. Windows Server, Linux, Network, appliances, etc.).

(b) disable terminated users or inactive accounts, in accordance with UNHCR policies;

(c) identify and report to UNHCR policy violations originating from administrative IDs (e.g., login violations, resource access violations, etc.);

(d) identify and report to UNHCR systematic attacks (e.g., attempts to logon, etc.); and

(e) provide logs of security events containing sufficient data to support security audits (e.g., audits of security effectiveness and compliance, etc.).

2.8. Security Assessment and Audit Support

Security Assessment and Audit Support Services are those activities associated supporting UNHCR security assessments, internal audits and external audits.

Contractor Shall:

(a) Provide support for assessments and audit activities to identify control or security gaps (e.g., process documentation, data collection, report generation)

(b) provide a coordinator to support security assessments and audit activities when requested;

(c) maintain documentation required to support security assessments, audits, internal controls, and control testing;

(d) develop plans to remediate assessment and audit findings that do not comply with the established UNHCR policies and requirements related to security; and

(e) implement remediation plans upon UNHCR approval.

3 *Implementation of Security Services*

Contractor shall:

(a) Be actively involved in the development of new desktop security services. Such new services shall be added to the Services in accordance with the Change Control Procedure; and

(b) follow the agreed ICT Project and Governance process in the delivery of new services. Contractor shall be involved in all aspects of the service development and will provide work and cost estimates as part of the approval process.

4 Out of Scope Security Services

The Parties agree that the following services are not within the scope of the Services defined within this Schedule 9:

(a) UNHCR security policy development;

(b) physical security at UNHCR facilities;

(c) approvals for Software/OS security patches; and

(d) licensing for UNHCR security tools.